Penerapan *Secret Image Sharing* Menggunakan Steganografi dengan Metode *Dynamic Embedding* dan *Authentication-Chaining*

Arya Widyadhana, Muchammad Husni, Rully Soelaiman
Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111
E-mail: husni@its.ac.id

***Abstrak*—Teknik yang banyak digunakan untuk menyebarkan suatu citra rahasia kepada *n* orang adalah dengan cara membagi citra rahasia ke dalam beberapa bagian yang kemudian diproses menggunakan skema (*k*, *n*)-Shamir *Secret Sharing* yang dikemukakan oleh Adi Shamir (1979). Bagian-bagian dari citra rahasia yang sudah diproses tersebut disisipkan ke dalam *n* citra kamuflase dan menghasilkan *n* citra stego. Penyisipan dilakukan sedemikian rupa sehingga kualitas visual citra stego semirip mungkin dengan citra kamuflase. Cara untuk memproteksi citra stego dari orang yang tidak berhak adalah dengan cara menyisipkan suatu bit otentikasi yang berfungsi sebagai suatu *digital signature* dari citra stego. Citra rahasia dapat dirangkai kembali jika terdapat minimal *k* citra stego asli. Teknik ini dinamakan *Secret Image Sharing*.**

***Kata Kunci*—Citra Stego, Otentikasi, Secret Image Sharing, Steganografi.**

I. PENDAHULUAN

SECRET image sharing adalah suatu teknik untuk menyebarkan suatu citra rahasia kepada *n* orang dengan menggunakan skema (*k*, *n*)-*Secret Sharing* yang dikemukakan oleh Adi Shamir [1]. Citra rahasia dibagikan dan disisipkan ke dalam *n* citra kamuflase untuk menghasilkan *n* citra stego. Citra rahasia dapat dirangkai kembali dengan menggunakan minimal *k* citra stego. Ada dua teknik untuk menyisipkan suatu citra rahasia ke dalam citra kamuflase yaitu menggunakan steganografi atau enkripsi [2]. Di dalam tulisan ini, teknik yang akan digunakan untuk penyisipan adalah steganografi.

Banyak penelitian yang dilakukan untuk menemukan cara paling aman dan efisien untuk *Secret Image Sharing*. Namun beberapa permasalahan muncul seperti ukuran citra stego yang terlalu besar, kualitas visual citra stego yang kurang bagus, dan metode otentikasi yang kurang aman.

Ukuran citra stego yang dihasilkan pada penelitian-penelitian sebelumnya besar. Ini disebabkan oleh penyisipan statis dimana penyisipan dilakukan ke dalam blok-blok piksel dengan ukuran empat piksel per blok. Ini menyebabkan citra stego berukuran minimal empat kali lebih besar dari citra rahasia [3].

Kualitas visual citra stego yang dihasilkan pada penelitian-penelitian sebelumnya kurang bagus karena penyisipan dilakukan secara statis dan ini menimbulkan kemungkinan dimana hanya sebagian citra kamuflase yang digunakan untuk penyisipan dan bagian yang lain tetap. Ini menyebabkan nilai piksel-piksel pada citra stego yang digunakan untuk penyisipan dengan nilai piksel-piksel yang tidak digunakan untuk penyisipan berbeda jauh jika dibandingkan dengan nilai piksel-piksel pada citra kamuflase. Ini jelas akan menurunkan kualitas visual dari citra stego [4].

Metode-metode otentikasi yang selama ini dikembangkan, yang muncul sebagai yang terbaik adalah yang dikemukakan Chang [2] dengan probabilitas mendeteksi suatu citra stego palsu sebesar 15/16. Tetapi jumlah bit yang digunakan untuk otentikasi sebanyak empat yang masih terlalu banyak karena dapat menurunkan kualitas visual citra stego.

Dalam tulisan ini akan dikembangkan suatu metode penyisipan dinamis untuk mengatasi masalah yang muncul akibat penyisipan statis pada penelitian-penelitian sebelumnya. Selain itu akan dikembangkan suatu metode otentikasi yang dapat mencapai probabilitas yang sama dengan metode milik Chang tetapi hanya menggunakan dua bit otentikasi.

II. METODE

A. *Shamir Secret Sharing*

Shamir *Secret Sharing* adalah sebuah metode yang digunakan untuk memecah suatu nilai rahasia kepada n orang dimana setiap orang mendapat sebuah nilai unik yang dihasilkan dari sebuah perhitungan [1]. Untuk dapat mengetahui kembali nilai rahasia dibutuhkan minimal k nilai unik dari n orang tersebut dimana k kurang dari n.

$$F(x) = y + m_1 \times x + m_2 \times x^2 + \cdots + m_{k-1} \times x^{k-1} \quad (1)$$

y adalah nilai rahasia. $m_1, m_2, \ldots, m_{k-1}$ adalah integer positif sembarang. Dari perhitungan diatas, setiap orang i mendapat sebuah pasangan nilai $(x_i, F(x_i))$ yang disimpan untuk mendapatkan kembali nilai rahasia. Nilai x_i untuk setiap orang harus unik dengan yang lain. Untuk mendapatkan kembali nilai y maka digunakan rumus polinomial Lagrange sebagai berikut:

$$y = (-1)^{k-1}\left[F(x_1)\frac{x_2 x_3 \ldots x_k}{(x_1 - x_2)(x_1 - x_3)\ldots(x_1 - x_k)} + F(x_2)\frac{x_1 x_3 \ldots x_k}{(x_2 - x_1)(x_2 - x_3)\ldots(x_2 - x_k)} + \ldots + F(x_k)\frac{x_1 x_2 \ldots x_{k-1}}{(x_k - x_1)(x_k - x_2)\ldots(x_k - x_{k-1})}\right] \quad (2)$$

B. Secret Image Sharing

Untuk dapat menerapkan Shamir *Secret Sharing* pada *Secret Image Sharing*, maka citra kamuflase dibagi ke dalam blok-blok piksel sebanyak jumlah piksel pada citra rahasia. Nilai y pada Persamaan 1 adalah nilai salah satu piksel citra rahasia. Kemudian nilai x pada Persamaan 1 merupakan nilai piksel pertama pada blok piksel ke j pada citra kamuflase i [5]. Blok-blok piksel dihitung pada metode *Dynamic Embedding*. Karena nilai x pada Persamaan 1 untuk setiap orang harus unik maka jika ditemukan nilai x_{ij} pada citra kamuflase i dan blok ke j ada yang sama dengan nilai x_{ij} pada citra kamuflase yang lain, salah satu nilai x_{ij} ditambah atau dikurangi satu. Mengurangi atau menambahkan nilai suatu piksel dengan satu tidak akan terlalu berpengaruh pada citra karena mata manusia tidak bisa membedakan perubahan warna yang terjadi pada piksel tersebut [5].

Pada Persamaan 1 nilai yang dihasilkan bisa melebihi 255 sehingga tidak dapat direpresentasikan ke dalam satu *byte* dan oleh sebab itu nilai yang dihasilkan tidak dapat disisipkan ke dalam suatu piksel pada citra dengan tipe data tingkat keabuan. Oleh karena itu harus ada suatu penyesuaian Persamaan 1 terhadap kebutuhan pada implementasi *Secret Image Sharing*. Penyesuaian yang dilakukan adalah dengan cara hasil dari Persamaan 1 dimodulo dengan suatu bilangan q sehingga bilangan yang dihasilkan memiliki nilai diantara $0-(q-1)$. Bilangan q harus merupakan sebuah bilangan prima agar hasil modulo tidak ambigu. Bilangan prima terdekat dengan 255 adalah 251 sehingga jika dimodulo dengan 251, hasil dari Persamaan 1 memiliki nilai diantara $0-250$ [5]. Sehingga persamaan yang digunakan untuk *Secret Image Sharing* adalah sebagai berikut:

$$F(x) = y + m_1 \times x + m_2 \times x^2 + \cdots + m_{k-1} \times x^{k-1}{}_{mod\ 251} \quad (3)$$

Untuk menyesuaikan dengan Persamaan 3, maka semua nilai y, x, dan m harus bernilai dibawah 251 sehingga jika terdapat piksel dengan nilai 251 ke atas maka nilai piksel tersebut akan dirubah menjadi 250. Ini tidak akan terlalu berpengaruh pada kualitas visual dari suatu citra karena nilai piksel tingkat keabuan 250 – 255 terlalu terang untuk bisa dibedakan oleh mata manusia [5]. Penyesuaian yang dilakukan terhadap Persamaan 2 juga sama yaitu dengan cara menambahkan operasi modulo seperti pada Persamaan 3 sehingga menghasilkan persamaan sebagai berikut:

$$y = (-1)^{k-1}\left[F(x_1)\frac{x_2 x_3 \cdots x_k}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_k)} + F(x_2)\frac{x_1 x_3 \cdots x_k}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_k)} + \cdots + F(x_k)\frac{x_1 x_2 \cdots x_{k-1}}{(x_k-x_1)(x_k-x_2)\cdots(x_k-x_{k-1})}\right]_{mod 251} \quad (4)$$

C. Dynamic Embedding

Dynamic Embedding adalah suatu metode steganografi untuk menyisipkan bit-bit nilai piksel dari citra rahasia ke dalam *least significant bits* dari piksel-piksel pada citra kamuflase [4]. Penyisipan dilakukan ke dalam blok-blok piksel pada citra kamuflase yang ukuran tiap bloknya dihitung dengan cara:

$$BS = \left\lfloor \frac{|CI|}{l} \right\rfloor \quad (5)$$

BS adalah ukuran blok, CI adalah jumlah piksel dalam citra kamuflase dan l adalah jumlah piksel dalam citra rahasia. Kemudian jumlah bit yang akan disisipkan (Nb) pada setiap blok dihitung. Pada setiap D_i jumlah bit adalah sebanyak $8+m$ bit otentikasi dimana m bernilai 1, 2, atau 3.

$$Nb = \frac{|D_i|}{BS} \quad (6)$$

Dalam satu blok piksel sudah pasti $\lfloor Nb \rfloor$ bit digunakan untuk penyisipan tetapi jika Nb bukan sebuah integer maka dalam $|D_i| - BS \times \lfloor Nb \rfloor$ piksel terakhir dari blok tersebut bit yang digunakan untuk penyisipan adalah sebanyak $\lceil Nb \rceil$. Maka bit yang digunakan untuk penyisipan pada setiap piksel B_i pada blok B yang dilambangkan Ub_i adalah sebanyak:

$$Ub_i = \begin{cases} \lceil Nb \rceil, & jika\ i = 1, \ldots, BS \times |Nb| - |D_i| \\ \lfloor Nb \rfloor, & jika\ lainnya \end{cases} \quad (7)$$

D. Authentication-Chaining

Diperlukan suatu bit otentikasi yang dapat mendeteksi jika ada seseorang yang mengganti bit-bit pada citra stego. Metode yang dipakai juga harus menghasilkan suatu susunan bit-bit otentikasi yang susah ditebak oleh orang lain sehingga citra palsu atau citra stego yang telah diubah tidak akan melewati fase verifikasi pada saat merangkai kembali citra rahasia [4]. Metode yang digunakan adalah *Authentication-Chaining*.

Misalkan $B^j = \left(B_1^j, \ldots, B_{BS}^j\right)$ adalah blok ke *j* dari CI_i dan misalkan SH_i^j adalah nilai piksel pertama yang digunakan sebagai nilai x pada Persamaan 3 pada blok B^j. Maka bit otentikasi dari B^j yang dilambangkan Aut_i^j dihitung dengan sebuah *hash function* sebagai berikut:

$$Aut_i^j = XOR\langle H_k(SH_i^{j-1} \| SH_i^j \| \langle B_2^j \rangle_{M1} \| \langle B_3^j \rangle_{M2} \| \ldots \| \langle B_{BS}^j \rangle_{BS} \| j) \rangle_2 \quad (8)$$

B_k^j adalah bit-bit pada blok ke j dan piksel ke k yang tidak digunakan untuk penyisipan. $M_{k_{2 \le k \le BS}} = 8 - Ub_k$ adalah jumlah bit yang masih orisinil atau yang tidak digunakan untuk penyisipan dari blok B_k^j. SH_i^0 bernilai 0.

III. HASIL DAN PEMBAHASAN

A. Peak Signal-to-Noise Ratio (PSNR)

Untuk mengukur kualitas atau kemiripan dari citra stego dibandingkan dengan citra kamuflase, digunakan sebuah *Peak Signal-to-Noise Ratio* (PSNR) [5]. PSNR dihitung dengan cara:

$$PSNR = 10 \times log_{10}\frac{(255)^2}{MSE} dB \quad (9)$$

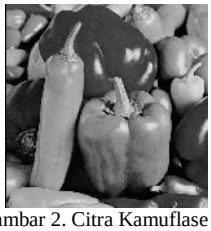
MSE adalah *mean-square error* antara citra kamuflase dengan citra stego. Jika citra kamuflase memiliki ukuran $f \times g$ maka MSE didefinisikan sebagai berikut:

$$MSE = \frac{1}{f \times g}\sum_{i=1}^{f}\sum_{j=1}^{g}(x_{ij} - y_{ij})^2 \quad (10)$$

Gambar 1. Citra Rahasia 256x256 Airplane

a) b)

c) d)



Gambar 2. Citra Kamuflase 512x512, a) Lena, b) Baboon, c) Pepper, d) Barbara

B. *Skema (k, n) untuk (2, 3)*

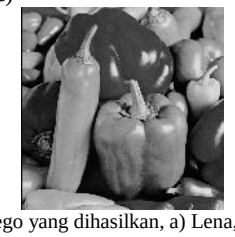
Uji coba yang dilakukan adalah menerapkan *Secret Image Sharing* dengan $n = 3$ dan $k = 2$ untuk dijadikan input pada Persamaan 3. Kemudian *Peak Signal-to-Noise Ratio* masing-masing citra stego dihitung. Hasil *Peak Signal-to-Noise Ratio* ditunjukkan pada Tabel 1.

Tabel 1.
Perbandingan *Peak Signal-to-Noise Ratio* Citra Stego Dengan Metode-Metode yang Berbeda Untuk Skema (3, 2)

Metode	PSNR (dB)		
	Lena	Pepper	Baboon
Lin-Tsai	42,29	42,27	42,28
Chang	44,62	44,58	44,57
Yang	40,52	40,25	40,21
Metode penelitian ini	48,18	48,12	48,10

a) b)

c)



Gambar 3. Citra stego yang dihasilkan, a) Lena, b) Baboon, c) Pepper

C. *Skema (k, n) untuk (3, 4)*

Uji coba yang dilakukan adalah menerapkan *Secret Image Sharing* dengan $n = 4$ dan $k = 3$ untuk dijadikan input pada Persamaan 2.3. Kemudian *Peak Signal-to-Noise-Ratio* masing-masing citra stego dihitung. Hasil *Peak Signal-to-Noise Ratio* ditunjukkan pada Tabel 3.

Tabel 2.
Perbandingan *Peak Signal-to-Noise Ratio* Citra Stego Dengan Metode-Metode yang Berbeda Untuk Skema (3, 4)

Metode	PSNR (dB)			
	Lena	Pepper	Baboon	Barbara
Lin-Tsai	44,66	44,63	44,65	44,73
Chang	46,97	46,95	46,93	46,89
Yang	42,70	42,09	42,30	41,68
Metode penelitian ini	51,94	51,93	51,93	51,90

a) b)

c) d)

Gambar 4. Citra stego yang dihasilkan, a) Lena, b) Baboon, c) Pepper, d) Barbara

D. *Pendeteksian Citra Stego Palsu*

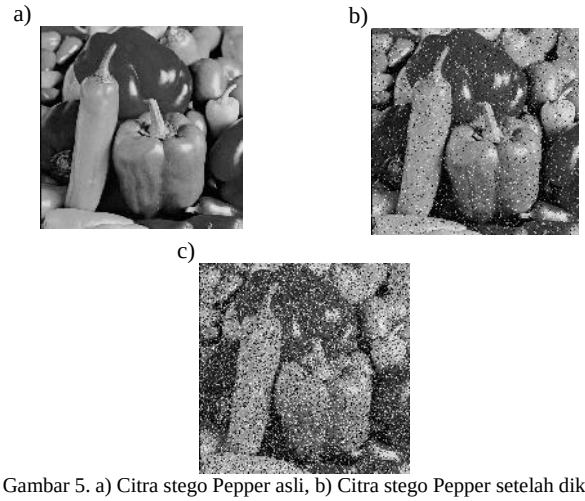
Uji coba yang dilakukan adalah mengubah salah satu bit otentikasi pada salah satu blok piksel pada citra stego untuk mengetahui apakah proses otentikasi berhasil. Dipilih secara acak blok piksel pada citra stego dan salah satu bit otentikasi pada blok piksel tersebut diubah. Kemudian diuji coba apakah citra stego yang diubah bit otentikasinya terdeteksi sebagai suatu citra stego palsu pada fase verifikasi. Proses ini diulang sebanyak 20 kali untuk kemudian dicatat apakah berhasil atau tidak citra stego yang sudah diubah bit otentikasinya terdeteksi.

Ternyata pada setiap fase verifikasi, citra stego terdeteksi sebagai sebuah citra stego palsu. Ini membuktikan bahwa metode *Authentication-Chaining* memiliki probabilitas sebesar 2^{-2a} untuk sebuah citra stego, yang sudah diubah-ubah bit-bit pikselnya, melewati fase verifikasi dengan menggunakan 2 bit otentikasi.

E. *Pendeteksian Citra Stego Melalui Kanal yang Memiliki Noise*

Pada simulasi pengiriman citra stego melalui kanal dengan *noise* sebesar 5%, ternyata citra stego yang diubah nilai bit-bitnya dianggap sebagai suatu citra stego yang rusak. Sehingga citra rahasia tidak dapat dirangkai kembali. Kesimpulan yang dapat diambil adalah jika citra stego dikirim

melalui sebuah kanal *noisy*, asal tidak lebih dari $n-k$ citra stego rusak akibat *noise* yang terdapat pada kanal tersebut, maka citra rahasia masih dapat dirangkai kembali. Tetapi jika lebih dari $n-k$ citra stego rusak akibat *noise* yang terdapat pada kanal tersebut, maka citra rahasia tidak dapat dirangkai kembali.



Gambar 5. a) Citra stego Pepper asli, b) Citra stego Pepper setelah dikirim melalui kanal yang memiliki noise sebesar 5%, c) Citra stego Pepper setelah dikirim melalui kanal yang memiliki noise sebesar 20%

IV. KESIMPULAN

Penelitian ini berhasil mengkonfirmasi bahwa *Secret Image Sharing* menggunakan steganografi dengan metode *Dynamic Embedding* menghasilkan citra stego yang kualitas visualnya lebih baik daripada hasil citra stego dengan menggunakan metode-metode pada penelitian-penelitian sebelumnya. Nilai *Peak Signal-to-Noise Ratio* citra stego yang dihasilkan oleh metode *Dynamic Embedding* selalu lebih tinggi daripada citra stego yang dihasilkan metode lain.

Selain itu metode *Authentication-Chaining* yang dipakai untuk otentikasi citra stego, mampu memiliki probabilitas mendeteksi citra stego sebesar 2^{-2a} dengan menggunakan 2 bit otentikasi.

DAFTAR PUSTAKA

[1] A. Shamir, "*How to Share a Secret*," Communication of the ACM vol. 22, (1979) 612-613.

[2] C. Chang, Y. Hsieh, C. Lin, "*Sharing Secrets in Stego Images with Authentication*," Pattern Recognition vol. 41, (2008) 3130 – 3137.

[3] A. Cheddad, J. Condell, K. Curran, P. McKevitt, "*Digital Image Steganography: Survey and Analysis of Current Methods*," Signal Processing vol. 90, (2010)727 – 752.

[4] Z. Eslami, J. Zarepour Ahmadabadi, "*Secret Image Sharing with Authentication-Chaining and Dynamic Embedding*," The Journal of Systems and Software vol. 84, (2011) 803 – 809.

[5] C. Lin, W. Tsai, "*Secret Image Sharing with Steganography and Authentication*," The Journal of Systems and Software vol. 73, (2004) 405–414.